Applying the Risk Management Framework

Jenn Fabius

Christina Sames

April 2016

MITRE

Objectives

- **Describe foundational concepts for managing cybersecurity risk**
- **Examine the relationship between RMF and Systems Engineering (SE)**
- **Describe the RMF, its artifacts, six steps, and linkages with SE**
- **Explain the requirements for authorizing or re-authorizing an information system**

Definitions

Key Terms and Definitions

- **Risk**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- **Threat**
  - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

- **Vulnerability**
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source

Source: CNSSI No. 4009, *Committee On National Security Systems (CNSS) Glossary*, April 2015

Key Terms and Definitions

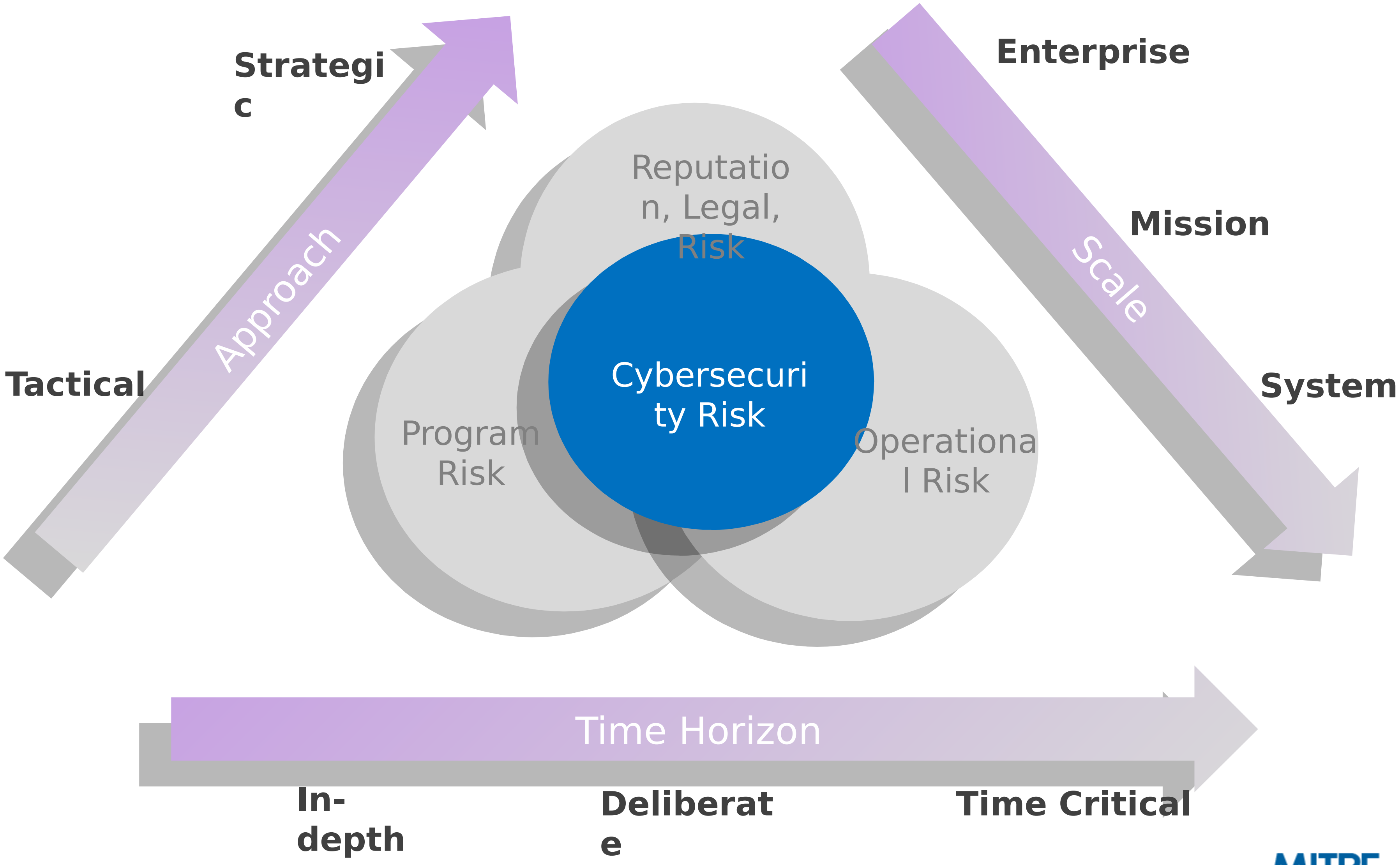
- **Cybersecurity (source: CNSSI No. 4009)**
  - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

- **Systems Engineering (source: INCOSE)**
  - Focuses on defining customer needs and required functionality, documenting requirements, and proceeding with system design while considering stakeholders' business and technical needs (source: INCOSE)
  - An engineering discipline who responsibility is creating and executing an interdisciplinary process to ensure that the customer and all other stakeholder needs are satisfied in a high-quality, trustworthy, cost-efficient, and schedule-compliant manner throughout a system's entire life cycle. (source: Draft NIST SP 800-160)

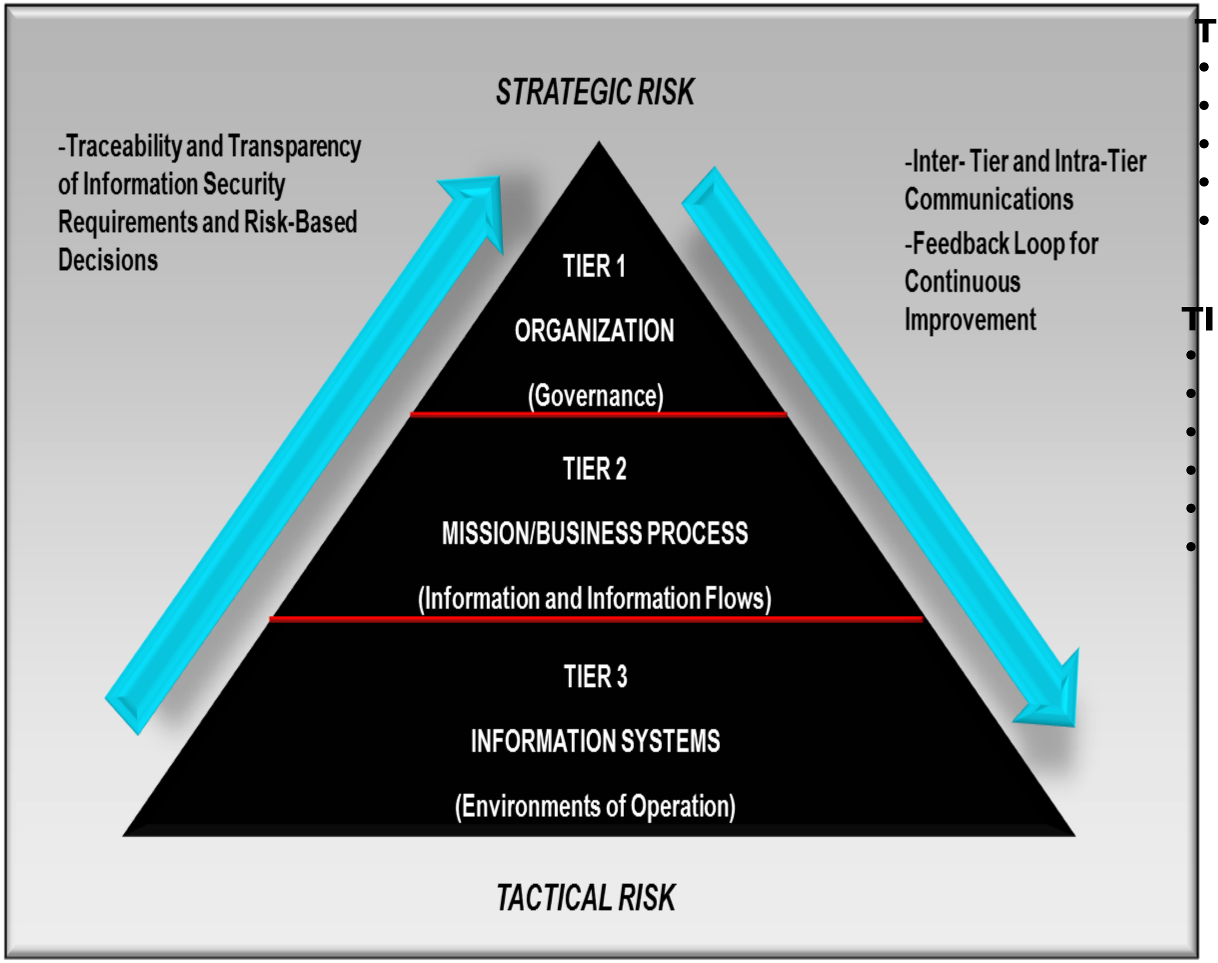
Risk…
Why manage it?

UM...HI, BOSS?...UH- REMEMBER THAT VIRUS EARLIER WE THOUGHT WAS RELATIVELY HARMLESS?
WELL...

Some Dimensions of Cybersecurity Risk



Developing a Enterprise-wide Risk Management Strategy



STRATEGIC RISK

-Traceability and Transparency of Information Security Requirements and Risk-Based Decisions

-Inter- Tier and Intra-Tier Communications

-Feedback Loop for Continuous Improvement

TIER 1

ORGANIZATION

(Governance)

TIER 2

MISSION/BUSINESS PROCESS

(Information and Information Flows)

TIER 3

INFORMATION SYSTEMS

(Environments of Operation)

TACTICAL RISK

TIER 1

- **Risk Executive Function**
- **Risk Assessment Methodologies**
- **Risk Mitigation Approaches**
- **Risk Tolerance**
- **Risk Monitoring Approaches**

TIER 2

- **Mission/Business Processes**
- **Information Flows**
- **Information Categorization**
- **Information Production Strategy**
- **Information Security Requirement**
- **Linkage to Enterprise Architectur**

TIER 3

- **Linkage to SDLC**
- **Information Security Categorization**
- **Selection of Security Controls**
- **Security Controls Allocation an Implementation**
- **Security Control Assessment**
- **Risk Acceptance**
- **Continuous Monitoring**

MITRE

Enterprise Level Risk Management and SE

- **Establishing risk awareness in order to achieve sufficient resiliency and continue to support the mission**
- **Considering redundancy in the information system and the organization**
- **Identifying connections among systems (e.g., common and hybrid security control considerations) and impacts to overall organization or to specific systems**

System level risk management and SE

- **System level risk guided by enterprise risk management and risk tolerance**
  - Use of risk management strategies, reporting, and requirements elicitations to identify stakeholder concerns and needs
- **Mission need and risk tolerance affect system development and deployment**
- **RMF and SE both consider risks through threats, vulnerabilities, and impacts.**
  - Are the risks considered similar?
  - How can the results support implementation?
  - How to consider or get guidance regarding trade space recommendations?

Risk Framing within the RMF Context

- Sets the stage or context for RM activities
- Organizational definitions and assumptions threats, vulnerabilities, consequences/impact, and the relationships among risk factors
- Identifies, characterizes, and provides representative examples of threats, vulnerabilities, and consequences/impacts
- Promotes a common terminology
- Provides basis for discussing and comparing risks across disparate mission/business areas
- Constraints such as financial, legal, regulatory, and/or contractual requirements on subsequent RM activities

Risk Tolerance within the RMF Context

- **Addresses identification of upper bound of willingness to accept risk within or across missions**
- **Involves:**
  - Risk appetite for specific types of losses/compromises
  - Subjective risk tolerance of senior leaders/executives in organizations
  - Influence of the organizational culture
  - Multiple and often competing priorities, leading to trade-offs and establishing priorities
- **Establishes priorities to make the best use of limited resources and minimize exposure:**
  - Range of risk types an organization faces
  - Degree of interconnection across the enterprise
  - Allocation of time and resources to minimize risk exposures
  - Determination of the types of risk that require immediate action

Risk tolerance levels must be defined

Risk Assessment within RMF context

- **Informs risk response activities**
- **Entails analysis conducted to identify threats and vulnerabilities as well as determine risks and uncertainties**
  - Related and influenced to risk assessment include root cause analysis, correlation of risk, and risk aggregation.
- **Requires analysis of threat, vulnerability, likelihood and impact to make risk determination**
  - Time horizon associated with risk occurrence.
- **When assessing risk, impacts refers to:**
  - Impacts to the missions or lines of business.
  - Impacts to stakeholders (i.e., the organization, other organizations, individuals, and the Nation).

Risk Response within RMF Context

- **Purpose**
  - Determine and implement actions required to manage risk to an acceptable level
- **Types of risk responses include:**
  - Risk acceptance
  - Risk avoidance
  - Risk mitigation
  - Risk transfer or sharing
- **Selected response(s) based on analysis of trade-offs between cost, impact, and tolerance level**
- **Frequently use more than one type of risk response in combination with a set of mitigations**
- **To be relevant, response requires action and follow-up**

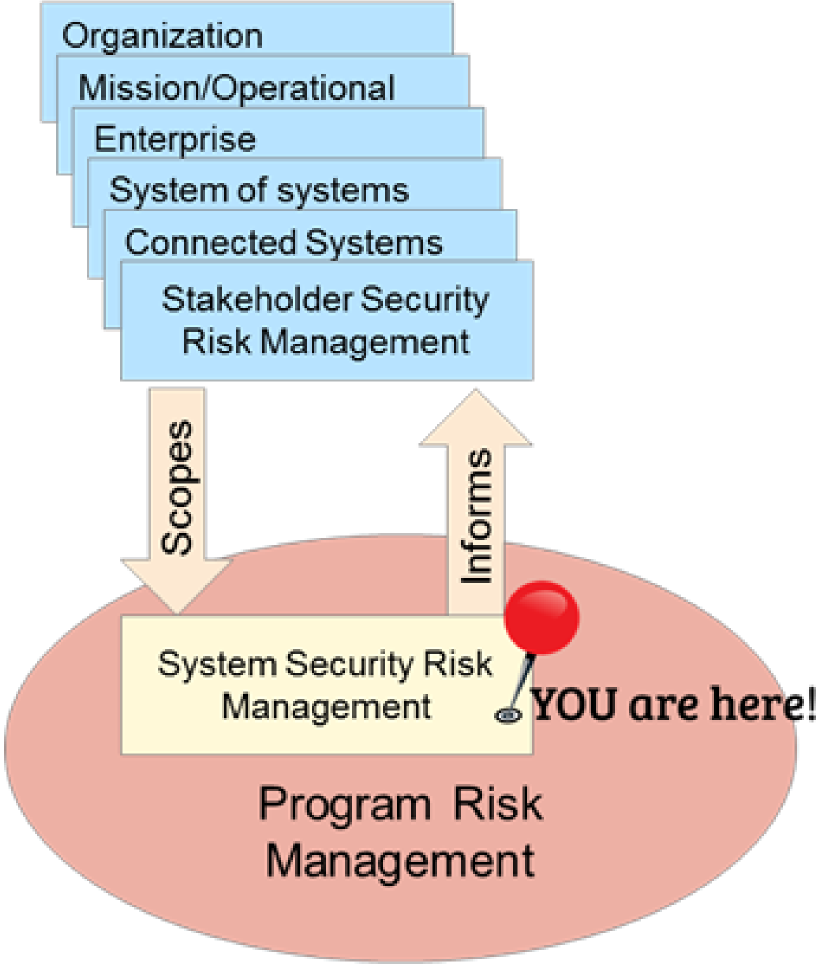
Risk Monitoring within RMF Context

- **Identify changes to:**
  - Systems
  - Environments
  - Mission
  - Technology
- **Three main reasons for monitoring:**
  1. Compliance
  2. Effectiveness
  3. Changes
- **Reason for monitoring and tier of operation will shape frequency of as well as how much is automated versus procedural**

Risk Analyses (SE perspective)

- **Analyzes and prioritizes risk**
  - Identify threats
  - Estimate likelihood
  - Consider stakeholder concerns and priorities
- **Generate alternatives for treatment**
- **Implement option and monitor for potential future modifications**

SE Team and Input to Risk Analyses



Security risk of one is a security risk shared

The relationship.. RMF and SE

Traditional System Lifecycle

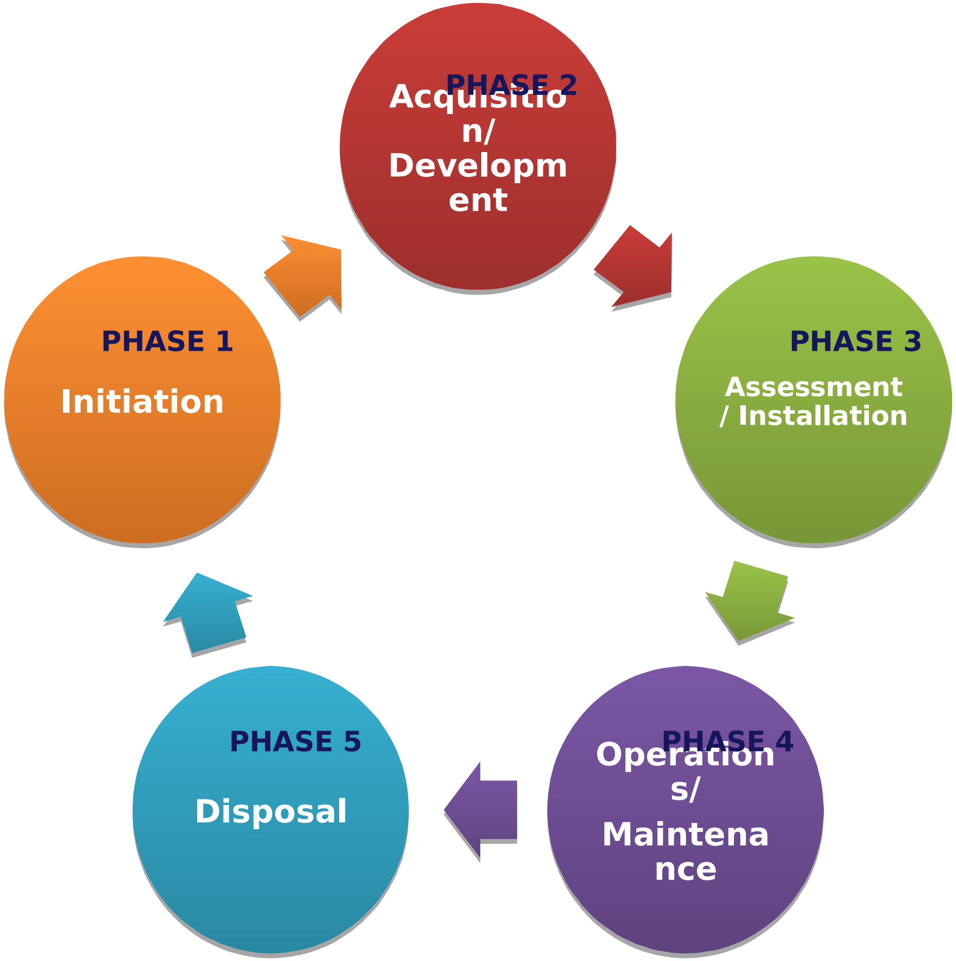
PHASE 1: The need for system is expressed and the system purpose and high level requirements are documented.

PHASE 2: System is designed, purchased, programmed, developed or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle of the acquisition cycle.

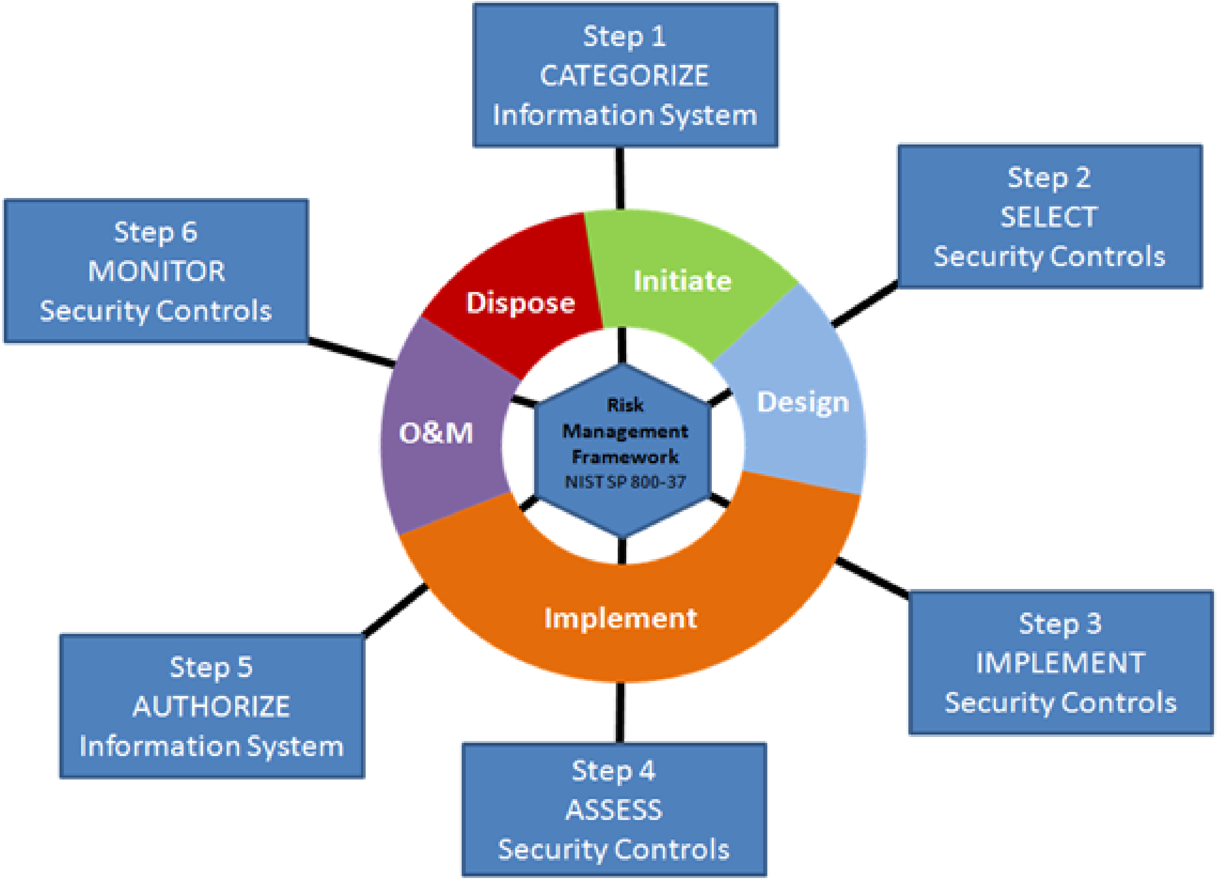
PHASE 3: After initial system testing, the system is installed or fielded.

PHASE 4: System performs the work for which it was developed.

PHASE 5: System is disposed of once the transition to a new computer system is completed.



RMF and the System Lifecycle



RMF and SE contribute to a holistic security perspective

- **RMF: Construct for near-real time decision making involving informed risk trades around cyber security.**
- **SE: Focus engineering efforts to ensure mission and business risk concerns are identified and addressed.**

Key Tenet: Risk can be managed; it cannot be avoided.

Where we see linkages: RMF and SE

- **RMF and SE may leverage the same data, technical management, and technical processes and their artifacts for different purposes**
- **SE informs RMF execution**
  - Authorizing Official and Security Control Assessor can leverage documents such as CONOPS, and Acquisition and Test & Evaluation Strategies to build RMF artifacts
- **RMF informs SE activities**
  - RMF authorization decisions and testing needs must be synced
- **RMF stakeholders must be included in any SE technical processes to ensure SE efforts reflect cybersecurity needs**
- **RMF and SE both focus heavily on risk management throughout the lifecycle**
- **Stakeholders in both SE and RMF have a tendency to focus on delivery of an end product – solution or authorization – and less on what happens afterwards**

Break

RMF in Detail

A way of looking at RMF Role Relationships

Enterprise View

Mission/Business View

Information System View

RMF Authorization Package

- System/Security Plan (SSP/SP)
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

System Security Plan (SSP)

- **Documents the security protection of the information system and describes the controls and critical elements in place or planned for**
  - Provides sufficient information to enable an understanding of the implementation of each security control in the context of the information system
  - Includes impact values for confidentiality, integrity, and availability of the information system
  - Reflects input from management responsible for the system, including the information system owner, information owners/data steward, information system security managers, and system administrator
  - Should be consistent with the enterprise architecture

May Be Incorporated into Other Engineering Documents

Security Assessment Report (SAR)

- **Ensures that Information System Owners and AOs maintain situational awareness**
  - Includes information related to security control effectiveness, system threats, system vulnerabilities, and other system security deficiencies
- **Documents both the initial assessment of security controls and the re-assessment of security controls as part the continuing monitoring process**
- **Provides information needed for reviewing findings to determine steps required to correct weaknesses identified for remediation**

Plan of Action and Milestones (POA&M)

- **Prepared by the Information System Owner or Common Control Provider for the Authorizing Official (AO)**
  - Serves as a repository for information about known weaknesses or deficiencies in an organizational program or in an information system
  - Describes the specific measure planned to:
    - Correct weaknesses/deficiencies noted in the security controls during the assessment; and
    - Address known vulnerabilities in the information system
- **Identifies:**
  - Tasks which need to be accomplished
  - Resources required to accomplish the elements of the plan
  - Any milestones in meeting the tasks, including scheduled completion dates

Authorization Decision Document

- **An Authorization Decision Document contains the authorization decision, terms and conditions for the authorization, and risk executive input (if provided)**
- **An authorization decision results in either an Authorization to Operate (ATO) or a Denial of Authorization to Operate (DATO)**
- **Considerations if a system receives an ATO:**
  - Should reduce or eliminate vulnerabilities unless they have been specifically accepted as part of a risk-based authorization decision
  - Need to monitor ongoing effectiveness of security controls given changes to mission, system, and its environments of operation
  - A POA&M is needed to monitor progress in correcting deficiencies and weaknesses
- **Considerations if a system receives a DATO:**
  - The AO/DAO deems the risk is unacceptable
  - Immediate steps cannot be taken to reduce risk to an acceptable level

Develop Monitoring Strategy

- **Develop early in the SDLC**
  - Can be included in the SSP
  - Is approved by the AO

- **Defines how changes to the informa system will be monitored, how secu impact analysis will be conducted, and the security status reporting requirements**
- **Should identify the security controls to be monitored, the frequency of monitoring, and the control assessment approach**
- **Ongoing monitoring of security controls using automated tools and supporting databases facilitates near real-time risk management for the information system**

RMF Snapshot

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

Select baseline security controls; apply tailoring guidance as needed based on risk assessment.

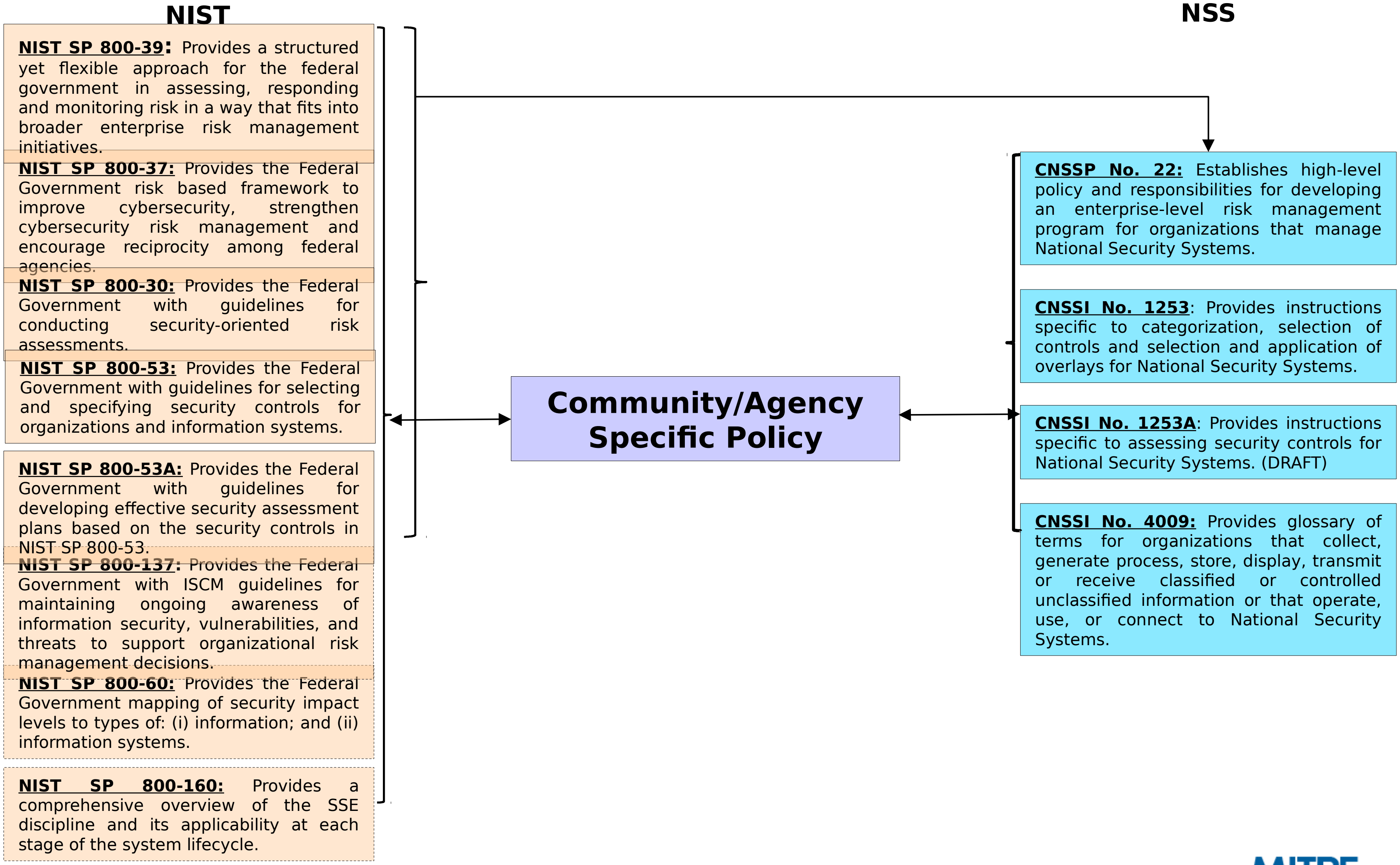
Implement security controls within enterprise architecture using sound systems engineering practices; apply security settings

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Continuously track changes to the information system that may affect security controls and reassess control effectiveness

RMF Snapshot



NIST

NSS

NIST SP 800-39: Provides a structured yet flexible approach for the federal government in assessing, responding and monitoring risk in a way that fits into broader enterprise risk management initiatives.

NIST SP 800-37: Provides the Federal Government risk based framework to improve cybersecurity, strengthen cybersecurity risk management and encourage reciprocity among federal agencies.

NIST SP 800-30: Provides the Federal Government with guidelines for conducting security-oriented risk assessments.

NIST SP 800-53: Provides the Federal Government with guidelines for selecting and specifying security controls for organizations and information systems.

NIST SP 800-53A: Provides the Federal Government with guidelines for developing effective security assessment plans based on the security controls in NIST SP 800-53.

NIST SP 800-137: Provides the Federal Government with ISCM guidelines for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

NIST SP 800-60: Provides the Federal Government mapping of security impact levels to types of: (i) information; and (ii) information systems.

NIST SP 800-160: Provides a comprehensive overview of the SSE discipline and its applicability at each stage of the system lifecycle.

Community/Agency Specific Policy

CNSSP No. 22: Establishes high-level policy and responsibilities for developing an enterprise-level risk management program for organizations that manage National Security Systems.

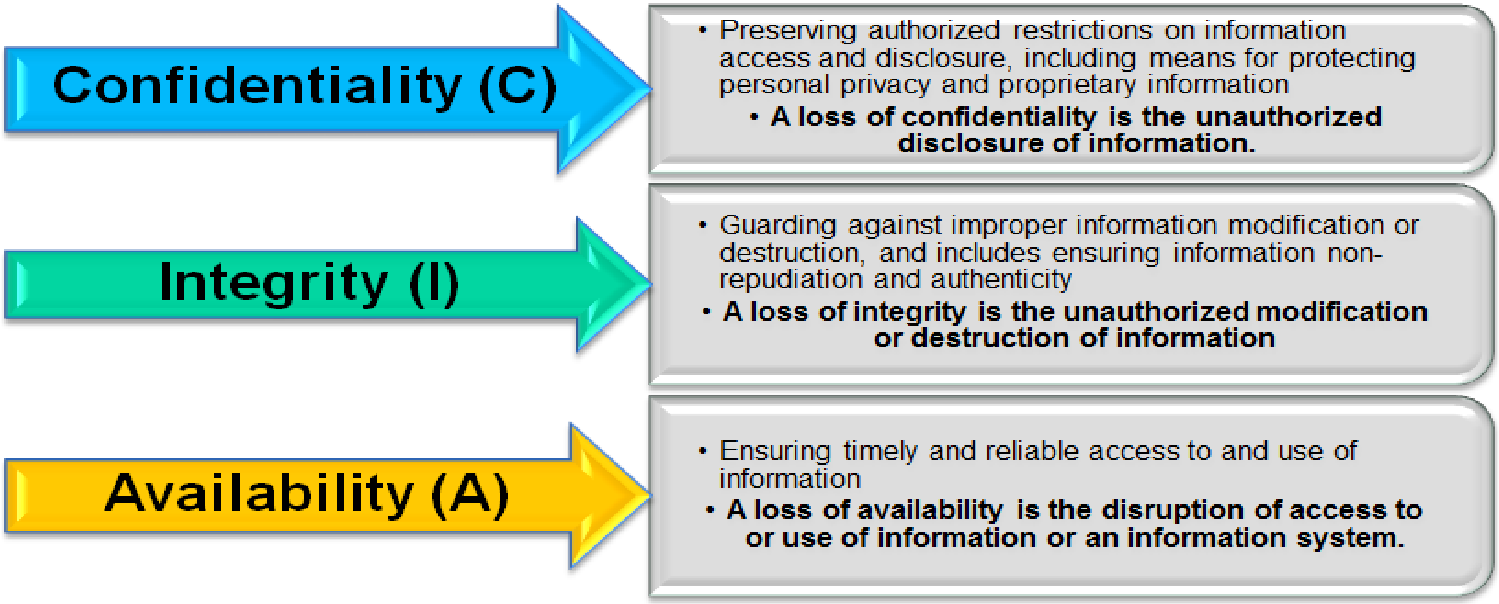
CNSSI No. 1253: Provides instructions specific to categorization, selection of controls and selection and application of overlays for National Security Systems.

CNSSI No. 1253A: Provides instructions specific to assessing security controls for National Security Systems. (DRAFT)

CNSSI No. 4009: Provides glossary of terms for organizations that collect, generate process, store, display, transmit or receive classified or controlled unclassified information or that operate, use, or connect to National Security Systems.

Determine Potential Impact Values

- **Potential impact values of Low (L), Moderate (M), or High (H) are:**
  - Assigned for information and information system
  - Based on the potential impact on organizations or individuals should a security breach occur for the three security objectives (C, I, and A) that are assigned for each identified information type



Confidentiality (C)

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
  - **A loss of confidentiality is the unauthorized disclosure of information.**

Integrity (I)

- Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **A loss of integrity is the unauthorized modification or destruction of information**

Availability (A)

- Ensuring timely and reliable access to and use of information
- **A loss of availability is the disruption of access to or use of information or an information system.**

How to Identify Information Types

- **An information type is a specific category of information defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.**
- **NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008) is the standard guidance for the identification of information types.**
  - As appropriat 0 with organization-

Security Category (System Impact Value) Determination

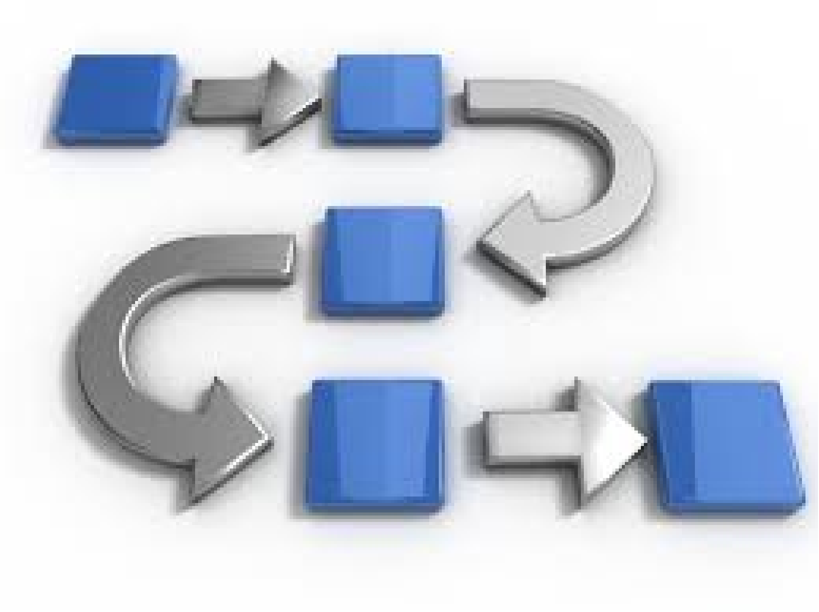
- **When information system contains multiple information types, determine the highest information type impact value to determine the system impact determination**

EXAMPLE

Information Type	C	I	A
Financial (Program Funding Sources)	M	M	M
Personally Identifiable Information (PII)	H	M	M
Health Information (HIPAA)	M	M	L
SYSTEM IMPACT VALUE	**H**	**M**	**M**

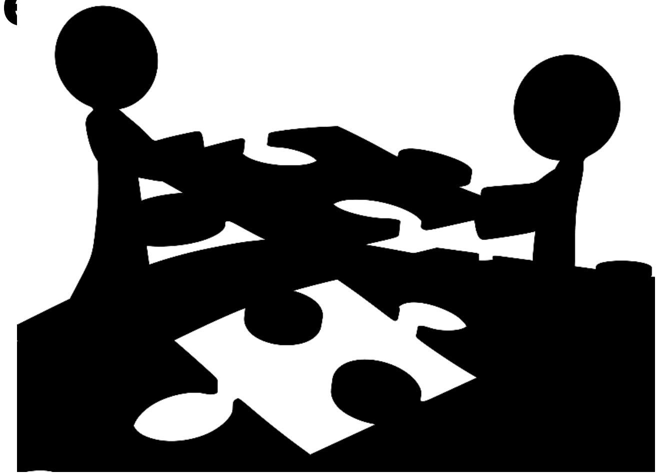
CNSSI No. 1253 Security Categorization Methodology

1) **Determine impact values**: i) for the **information types** processed, stored, transmitted, or protected by the information system; and ii) for the **information system**.
2) **Identify overlays** that apply to the information system and its operating environment to **account for additional factors (beyond impact)** that influence the selection of security contı



What is an overlay?

Both NIST SP 800-53 and CNSSI No. 1253 allow for the application of overlays, which are a specification of security controls, control enhancements, supplemental guidance, and other supporting information intended to complement (and further refine) security control baseline



Where we see linkages: Step 1 and SE

- Identifying the protection needs of an information system
- Understanding the security objectives
- Determining what is needed to protect an information system (addressing impact of loss and providing a secure system)
- Considering consequences of loss
- Considering value of the information when defining protection needs
- Categorizing system occurs both in Step 1 of RMF and during SE Concept Development

Security Control Selection Summary

1) **Select the baseline based on the categorization.**

   Civil agencies use NIST SP 800-53 baselines.

   NSS agencies use the CNSSI No. 1253 categorization approach and security control baselines.

2) **Apply any appropriate overlay(s) based on information and mission requirements**

3) **Tailor the initial security control set (combination of baseline and applicable overlay)**

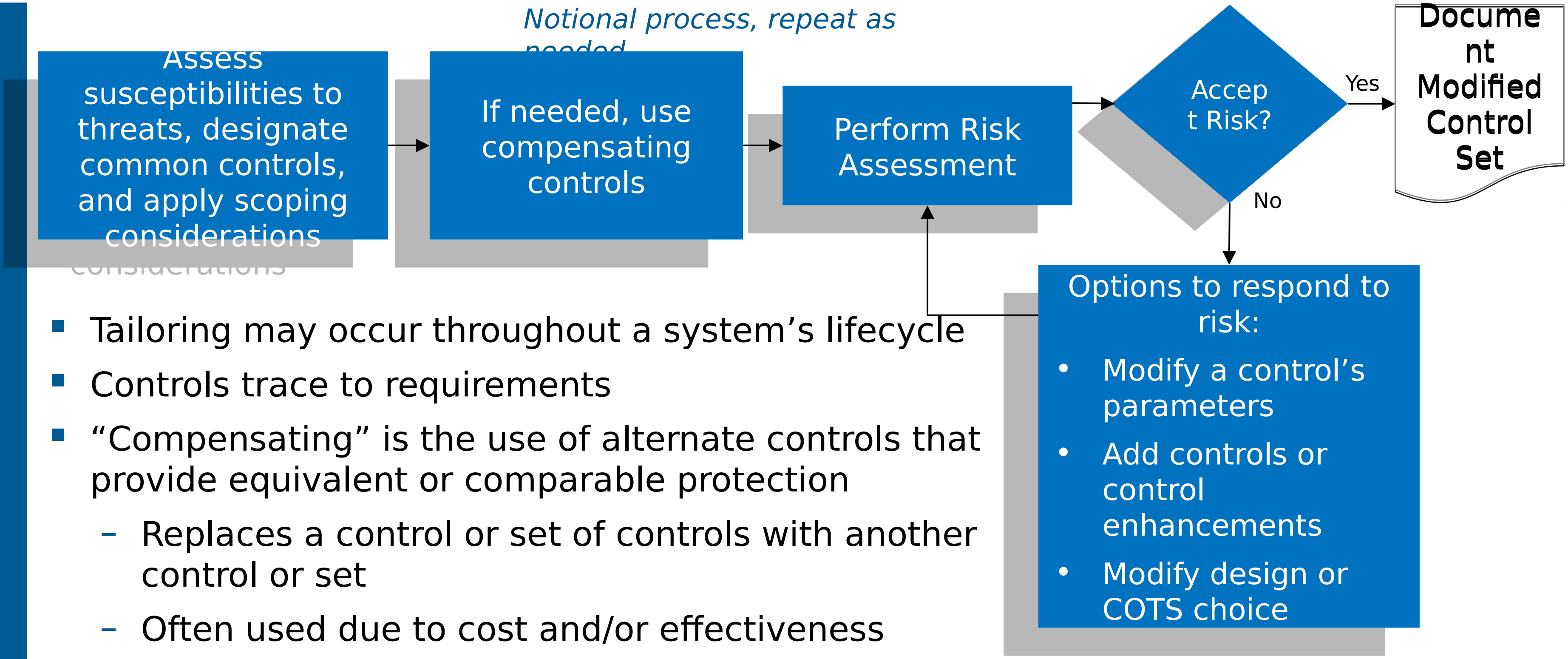
4) **Document the initial security control and any tailoring**

Using security controls

- **Using a security control set ensures the system has a comprehensive set(s) of security requirements and helps establish traceability**
- **Including systems engineers early and throughout RMF helps ensure:**
  - Tailoring of security controls
  - Identifying compensating security controls
  - Ensuring a strong justification for all security controls identified as applicable (beyond “because policy says so”)
  - A clear understanding of how a security considerations (e.g., malware, APT) can affect the execution/stand up of a system
  - Understanding of system risk management approach
  - Validating requirements and controls
    - Iterative process of controls helping refine requirements and requirements help identify controls that may be needed or not considered during original requirements identification

Tailoring Controls

Notional process, repeat as needed


Assess susceptibilities to threats, designate common controls, and apply scoping considerations
If needed, use compensating controls
Perform Risk Assessment
Accept Risk?
Yes
No
Document Modified Control Set

Options to respond to risk:

- Modify a control’s parameters
- Add controls or control enhancements
- Modify design or COTS choice

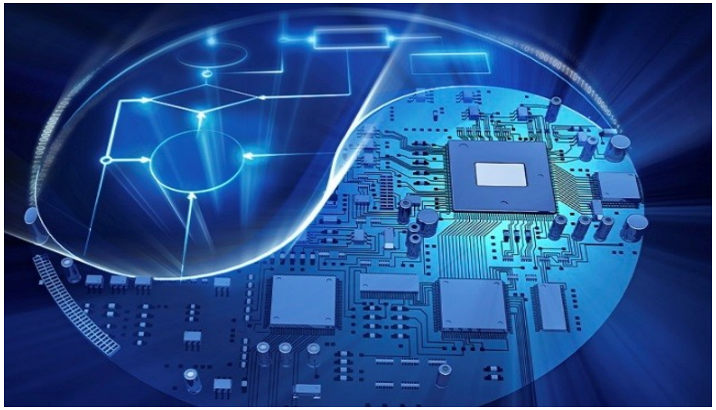
- Tailoring may occur throughout a system’s lifecycle
- Controls trace to requirements
- “Compensating” is the use of alternate controls that provide equivalent or comparable protection
  - Replaces a control or set of controls with another control or set
  - Often used due to cost and/or effectiveness reasons
- Residual risk not acceptable to the AO may be mitigated with adding controls or by enhancing existing controls, among other options

Common Security Controls

- **Can be inherited by one or more organizational information systems**
- **Provides potential cost savings for the organization**
- **Mandated use of common controls is one means to provide standardization across the organization**
- **Common controls should weigh into the documentation of the tailored control set – the first out ring**

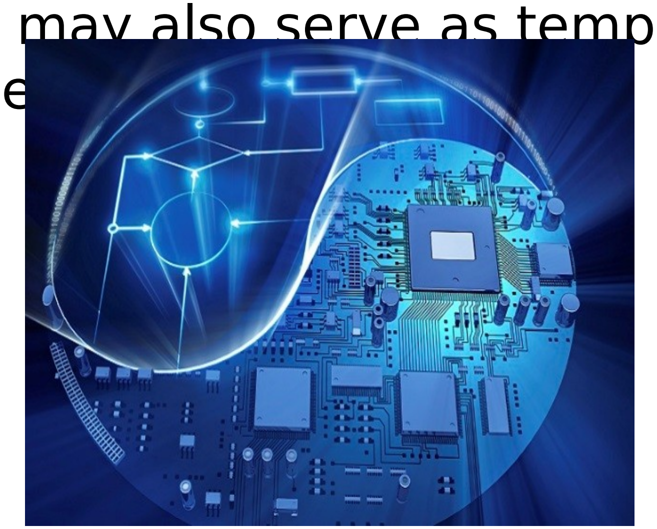
System-Specific Controls

- **Provide a security capability for a particular information system only**
  - System-specific controls are the primary responsibility of information system owners and their respective authorizing officials.



Hybrid Controls

- **Have both system-specific and common characteristics**
  - Organizations assign a hybrid status to a security control when one part of the control is deemed to be common and another part of the control is deemed to be system-specific.
  - Hybrid controls may also serve as templates for further control refineme

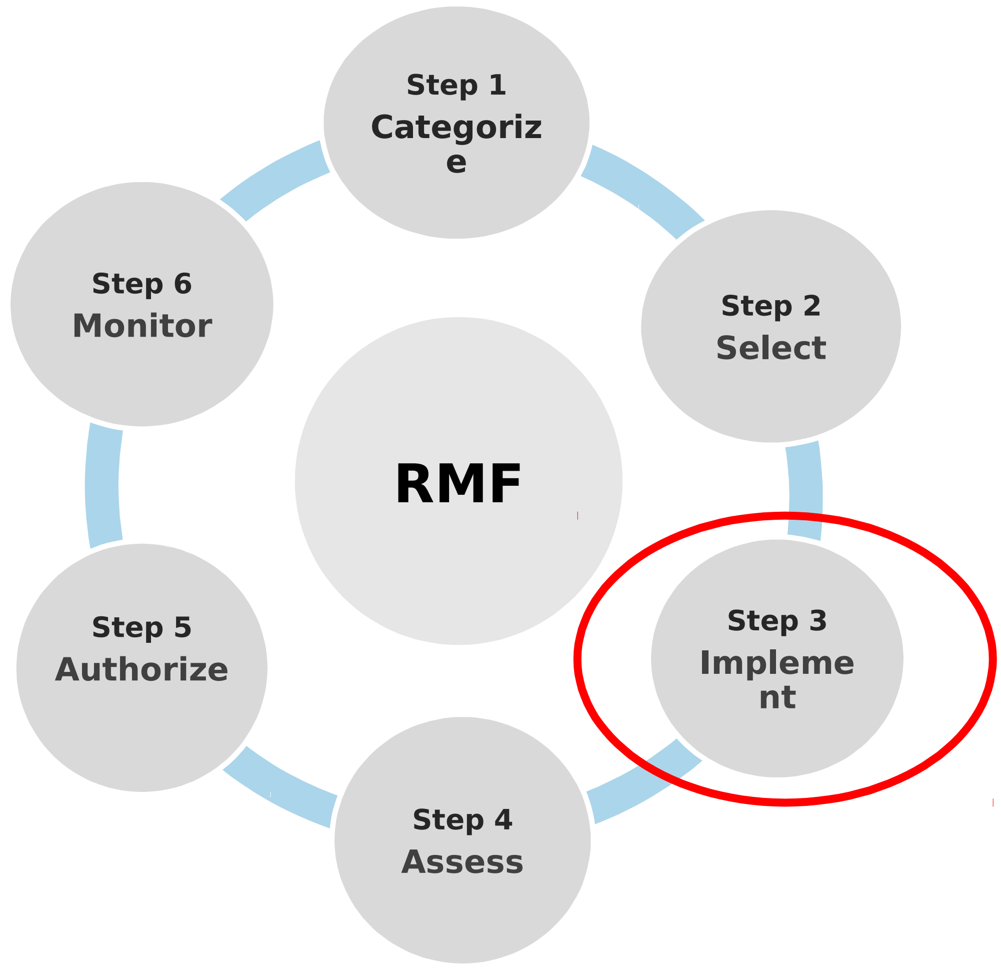


Compensating Security Controls

- **Compensating controls are safeguards or countermeasures employed in lieu of a security control recommended in the baseline that provides a comparable level of protection**
- **A variety of circumstances may require the use of compensating security controls:**
  - The selected control in the catalog cannot be applied to a given system
  - The selected control would impose excessive or unnecessary costs on the organization
  - The selected control may have a significantly adverse effect on mission requirements
- **When selecting compensating controls, the organization must:**
  - Select the compensating control from NIST SP 800-53, or adopt from another source
  - Tailor out the original control and list compensating control(s) as justification
  - Provide and document supporting rationale for how it delivers an equivalent security capability and why the related baseline security control could not be employed
  - Assess and formally accept the risk associated with employing the compensating control

Where we see linkages: Step 2 and SE

- **Security requirements are also identified as part of the SE stakeholders requirements definition and requirements analysis efforts**
- **The intent expressed as a need for a security control must be transformed into a set of security requirements**
- **Once security requirements are identified, they can be transformed into security controls where needed**
- **Traceability between security requirements and security controls is necessary**
- **None of this matters if security controls are being used in contexts and for purposes that are exclusively outside of systems engineering**


Step 1
Categoriz
e
Step 2
Select
Step 3
Impleme
nt
Step 4
Assess
Step 5
Authorize
Step 6
Monitor
RMF

Security Control Implementation Documentation

- Security control documentation describes how common, system-specific, and hybrid controls are implemented.
- Formalizes plans and expectations regarding the overall functionality of the information system.
- Allows for traceability of decisions taken prior to and after deployment of the information system.
- The level of effort expended on documentation of the information system is commensurate with the purpose, scope, and impact of the system with respect to organizational missions, business functions [illegible]s.

Where we see linkages : RMF Steps 1-3 and SE

- **SE concept, requirements, and architecture efforts will result in decisions and artifacts that support security control implementation**
- **SE risk assessments and trades can be used to fulfill or inform cyber security risk decisions**
- **SE requirements and architecture decisions can be used to refine or validate security controls tailoring decisions made in the RMF**
  - This may include use of compensating controls or the determination to not use controls
- **Security controls implementation is a part of the SE implementation process**
- **Validation of requirements and controls**

Break

Security Assessments within SDLC

- **Security assessments can be effectively carried out at various stages in the SDLC**
  - Increases confidence that the security controls employed within or inherited by an information system are effective in their application
- **Security assessments are also routinely conducted via continuous monitoring during the operations and maintenance phase of the life cycle**
  - May be performed by information system owners, common control providers, information system security officers, independent assessors, auditors, and Inspectors General
  - Ensures that security controls are effective and continue to be effective in the operational environment where the system is deployed

Assessment Preparation

- **The Security Assessment Plan provides the objectives for the security control assessment and a roadmap of how to conduct the assessment**
  - Purpose and scope of test
  - Documents required
  - Type of test
  - Tools for testing
  - Requirements for connectivity
  - Assessment readiness review

- **Organizations consider both the technical expertise and level of independence required in selecting security control assessors**
  - An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system

Where we see linkages: Step 4 to SE

- **Security control assessments must be integrated into the SE T&E strategies, planning, and test activities**
- **SE T&E procedures ensure requirements are traceable and implemented correctly**
  - Security control assessments verify and validate that security controls are implemented as intended
- **SE T&E results can support security control assessment reports and POA&M development**
- **Assessing security controls as part of the DT&E process is recommended**

Plan of Action and Milestones

- **Used to monitor progress in correcting weaknesses and reducing risk**
- **Organizations should define strategy for developing POA&Ms based on:**
  - Security category of the information system
  - Specific weaknesses or deficiencies in the IS security controls
  - Importance of the identified security control weaknesses or deficiencies
  - Organization’s proposed risk management approach to address the identified weaknesses or deficiencies in the security controls
  - Organization’s rationale for accepting certain weaknesses or deficiencies in the security controls

POA&Ms may be used to track all risk responses, not just mitigations!

Risk Determination

- **SAR and POA&M input to Risk Assessmei**
- **Update the Risk Assessment**
  - Reassess to determine residual risk
- **Shaping risk recommendation**
  - Residual risks as it aligns to the stated or actual risk tolerance
  - Guidance provided by organization with respect to accepting risk
  - Pre-existing conditions that drive to specific risk recommendation
- **Informs Authorization Decision along with accompanying artifacts**

Authorization Decision

- **Authorization decisions are based upon the content of the authorization artifacts, including inputs from the organization’s Risk Executive (function) and any additional documentation required by the AO**
- **The artifacts and/or BOE provides an AO with comprehensive information on the security state of the information system**
- **An authorization decision resu**
  - ATO
  - DATO

Authorization Approaches

- **Organizations can choose from three different approaches when planning for and conducting security authorization:**
  1. Single Authorizing Official
  2. Multiple Designated Authorizing Officials or Joint Authorization
  3. Leveraged Authc uthorization Letter)

Factors for (Re) Authorizing Systems

- **Organizational risk tolerance**
- **Overarching risk guidance**
- **Specific mission and business requirements**
- **Dependencies among information systems**
- **Other risks not directly associated with the information system**
- **Residual risk that requires a risk decision or treatment**
- **Terms and conditions for an information system to operate**
- **Effectiveness of safeguards implemented and any changes to system factors**
- **Results of security control assessments (conducted as part of authorization, ongoing authorization, or reauthorization)**
- **Content of RMF authorization package**

Ongoing Authorization

- **Provides the AO with sufficient knowledge of the current security state of the IS to determine whether continued operation is acceptable**
- **Occurs at the discretion of the AO**
- **Meets the following conditions:**
  - System has an initial ATO with a zero-base review of the system and has entered the operations/maintenance phase of the SDLC
  - ISCM program in place
- **Time-driven or event-driven**
  - Authorization termination date is reached
  - Significant change to an IS or its security sta

Where we see linkages: Step 5 and SE

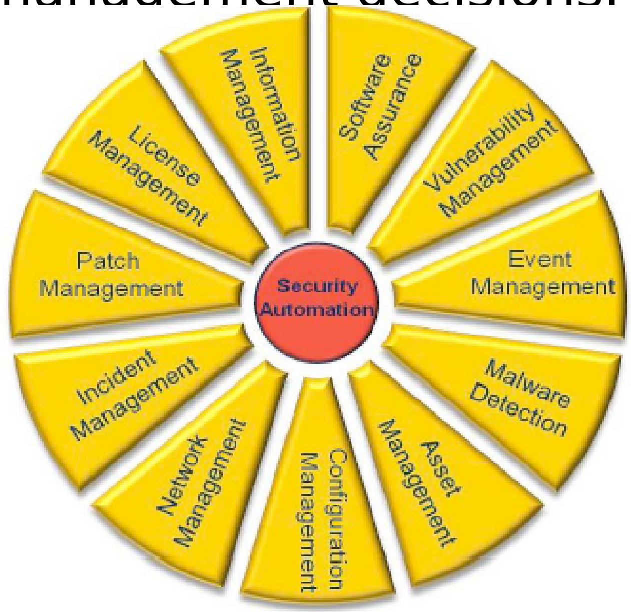
- **There is a stakeholder that must determine if a system is protected and secure enough to accept risks and operate based on residual risks**
- **Both RMF and SE determine what conditions would prompt change in system's operational status**
- **Communicating approval decision to other individuals within an organization (e.g., owners of interconnected systems)**
  - RMF risk decisions should be communicated through SE risk management, configuration management, and engineering review boards
- **Based on informed risk decision recommendations from artifacts developed by teams**
- **RMF authorization decisions support SE risk and opportunity decisions**

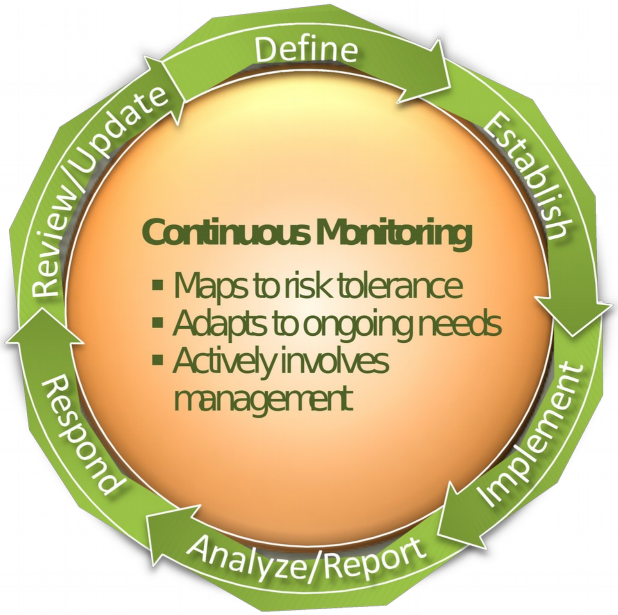
Monitoring

- **Certain events can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls.**
- **These events can include:**
  - An incident results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
  - A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified;
  - Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system; or
  - Significant changes to the organizational risk management strategy, information support or business functions, or informati sed, sto ed by the information system.

NIST SP 800-137

- **Definition for Information Security Continuous Monitoring from NIST SP 800-137, "Information Security Continuous Monitoring":**
  - “Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."



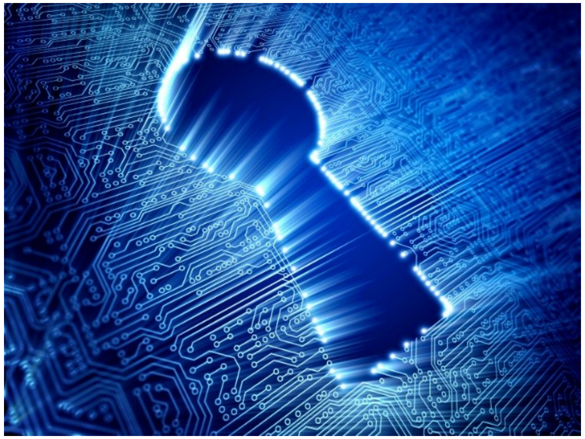


ISCM Supports More Efficient Assessments

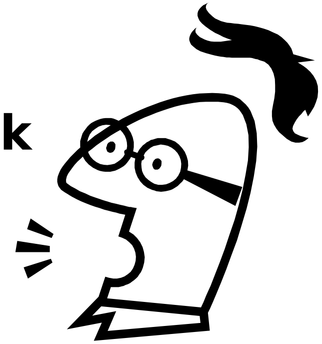
- **Results Aggregated into Reportable Metrics**
  - FISMA
  - OMB M-14-03
- **ISCM applications scan any/all environments (e.g., production, non-production)**
  - Differentiate Production and Non-Production Status
  - Optional “Potentially Destructive” Scans
    - Mainly Applicable to Application Scanners
    - Non-Destructive Scans Not Recommended In Production
- **Checks Applied on Servers/Applications/Endpoints**
  - Verified Against Defined Baselines
  - More Checks Executed More Frequently
  - Some Tools Support Customized Checks

What Does Monitoring Controls Mean?

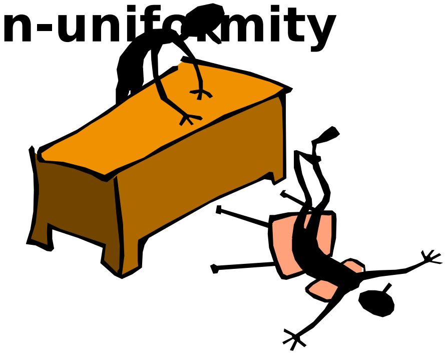
- **Assessing control effectiveness,**
- **Documenting changes to the system or its environment of operations,**
- **Conducting security impact analyses of the associated changes,**
- **Reporting the security state of the system to designated organizational officials,**
- **Performing ongoing risk determination and acceptance, and**
- **Conducting system removal and decommissioning when necessary**



ISCM Quickly Identifies Many Anomalies Encountered During Assessments



- **Accounts Without Passwords**
- **Allowing Root/Administrator Login Via Network**
- **Inactive/Never Active Privileged Accounts**
- **Unexpectedly Enabled Services**
- **Disabled Services “Enabled” by Patching**
- **Excessive World Write and Group Write Access (e.g., Replaced S/W Archives)**
- **Orphaned Files and Directories**
- **Unexpected Interface Changes**
- **System Configuration Inconsistency and Non-uniformity**
- **Lack of Baseline Definitions**
- **Auditing Misconfigurations (e.g., Events)**



Where we see linkages: Step 6 and SE

- Both consider the impacts of change to a system or the risks (system, mission, and environment) that affect operations
- Engineering trades support RMF continuous monitoring activities and enabling continuous monitoring may require trades
- Both address change to provide system operational and mission effectiveness
- Ongoing threat and vulnerability information inform risk management
- Security impacts affect ongoing system, operational, and mission upgrades and changes
- SE and RMF require integrated feedback loop to inform updates, modifications, and continuous improvements
- Monitoring needs may impact requirements definition process

Conclusion

What We Discussed Today

- **Foundational concepts for managing cybersecurity risk**
- **The relationship between RMF and SE**
- **The RMF, its artifacts, six steps, and linkages with SE**
- **Requirements for authorizing or re-authorizing an information system**

Contact Information

Jennifer Fabius
jfabius@mitre.org
703-983-3449

Christina Sames
csames@mitre.org
703-983-0161